International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 6, Issue 3, Jun 2016, 47-58
© TJPRC Pvt. Ltd.

TRANS STELLAR
• Journal Publications • Research Consultancy

A COMPREHENSIVE STUDY OF VARIOUS KINDS OF FRAUDS & IT'S IMPACT

NAVNEET KR. KASHYAP[1], B.K.PANDEY[2], H.L.MANDORIA[3] & ASHOK KUMAR[4]

[1]*Research scholar, Department of Information Technology, G.B.P.U.A & T, Pantnagar, India*

[2,4]*Assistant Professor, Department of Information Technology, G.B.P.U.A & T, Pantnagar, India*

[3]*Professor, Department Information Technology, G.B.P.U.A & T, Pantnagar, India*

ABSTRACT

This survey paper measures up and outlines from almost all released technological and examine content in intelligent fraud detection within the last 10 years. It characterizes the expert fraudster, formalizes the principle types of identified fraudulence, and provides the way of information confirmation gathered inside influenced commercial ventures. Contrasted with all related audits on misrepresentation recognition, this study covers a wonderful work more specialized articles and is the one and only, to the best of our insight, which proposes elective information and arrangements from related areas. Fraud detection includes checking the conduct of populaces of clients with a specific end goal to assess, identify, or stay away from undesirable conduct (Undesirable conduct is an expansive term including wrongdoing), interruption, and record defaulting. The objective of this paper is give complete investigation of various sorts of frauds and their discovery strategies.

***KEYWORDS:** Fraud, Fake, Fraud impact, Fraud Type, Bank & internet Fraud, Affected Industries*

Original Article

Received: May 20, 2016; **Accepted:** May 25, 2016; **Published:** May 30, 2016; **Paper Id.:** IJCSEITRJUN201605

INTRODUCTION

Felony detection is extremely intense occupation since its sorts and natures are very surprising and there's many ways. So for quite a while the conventional methods for information examination have been being used to recognize felony. They require intense and tedious errand that arrangements with various spaces of learning like business practices, fund, financial matters and law. Typically fraud detection can be comparable in appearance and content, however more often than not will be not indistinguishable. So fraud recognition is exceptionally intense assignment.

Fraud is a wrongful conduct. It includes misleading and deception with a specific end goal to profit. Double dealing could include fabricating fake MasterCard's or cushioning up protection claims, or making false claims to get contract advances you wouldn't have gotten something else. Fraud identification is a basic part of the measures executed for keeping up an assault tolerant database framework. In this paper, we take a perspective on various strategies and systems accessible to distinguish it too.

Fraud costs countless cash a year in harms and influences a huge number of individuals. Regrettably nobody is totally protected from being tricked. In any case, knowing how to perceive a fake, similar to a bank felony or a financial investment misrepresentation, will better help you secure yourself and your accounts. The intentions behind all these fraudulence plots, this paper is spread diverse sorts and subtypes of frauds.

WHAT IS A FRAUD?

Fraud is conscious misleading to secure unjustifiable or unlawful pickup, or to deny a casualty of a legitimate right. Fraud itself can be a common wrong (i.e., a Fraud injured party may sue the felony culprit to maintain a strategic distance from the felony and/or recoup financial remuneration), a criminal wrong (i.e., a Fraudster might be indicted and detained by legislative powers) or it might bring about no loss of cash, property or lawful right yet at the same time be a component of another common or criminal off-base. There are numerous words used to portray misrepresentation: Scam, con, cheat, blackmail, sham, deceive, fabrication, cheat, ploy, stratagem, dupe, certainty trap.

"Fraud is when dishonesty is utilized to pick up an exploitative point of interest, which is frequently money related, over someone else."

TYPES OF FRAUDS

Frauds can easily get classified through the kind of sufferer included. The most known organizations of targets experienced by researchers consist of:

- Dealers
- Loan Providers
- Companies
- Banking institutions or other financial institutions
- Central or localized authorities
- Fraud by influencing economic marketplace

Frauds will also be Listed by the Method or Procedure Utilized by the Fraudster. these Types of Fraud Consist of:

- Advanced cost frauds
- Fake bills
- Technology hacking of important information or property
- Decay and graft
- Counterfeiting, falsification, or copyright laws misuse
- Credit Card fraud
- Fake Accounting - handling of records and accountancy reports
- Counterfeit personal bankruptcy - victimization of cross-border business frameworks
- Insurance policies fraud
- Web internet based scams - sale, loan card purchases, financial investment scams
- Financial fraud

- Extended organization fraud
- Borrowing of assets
- Cash cleaning
- Home Finance Loan Fraud
- Paysheet fraud
- Major representatives - failing of systems to limit key people
- Great Pyramid schemes
- Unwanted document frauds.
- **CREDIT CARD FRAUD**

Shockingly, fraud is turning into a perpetually normal risk to customers - especially with regards to utilizing you MasterCard. Besides, demonstrate the cost of charge card misrepresentation is high - driving cardholders and Visa backers as much as 500 thousand a year.

Exchanges finished with charge cards appear to end up increasingly famous with the presentation of web shopping and managing an account. Correspondingly, the volume of charge card cheats has likewise expanded with the presentation of fresher innovation. From embossers to encoders to decoders, Visa forgers are currently utilizing the most recent innovation to peruse, change, and upload attractive data on fake charge cards.

TYPES OF CREDIT CARD FRAUD

Five different categories come inside Credit fraud:

- **Counterfeit Credit Card:** To make fake cards crooks utilize the most up to date innovation to "skim" data contained on attractive stripes of cards and to pass security components, for example, visualizations or holograms.
- **Misplaced or Swiped Cards:** Cards taken from their cardholders or lost by them represent 23% of all card cheats. Regularly, cards are stolen from the work environment, exercise center, and unattended vehicles.
- **No-Card Fraud:** Involves 10% of the considerable number of misfortunes and is finished without the physical card close by. This can happen by giving your charge card data on the telephone to shady telemarketers and misleading Internet locales that are advancing the offers of their non-existent products and administrations.
- **Non-Receipt Fraud:** It happens when new or supplanted cards sent by your card organization are stolen amid the procedure of being sent. In any kind of situation, this sort of felony is on the decay with the card-actuation handle that most organizations use.
- ***Identity-Theft Fraud:*** happens when hoodlums apply for a card utilizing another person' character and data.
- **INVESTMENT FRAUD**

Investment Fraud is any plan or duplicity identifying with speculations that influence a man or organization.

Investment felony includes:.

- **Illegitimate Insider Trading:** The expression "insider trading" can classify to lawful or unlawful exchanges. Insider trading is legitimate when commercial insiders authorities, professionals, and key workers buy and offer shares of their organization. The United States Securities and Exchanges Commissions (SEC) keep a record of all exchanges directed by corporate insiders.
- **Fake adjustment Of The Stock Market :** falsified control of the Stock Market happens principally when telemarketers or spammer use powerful procedures to paint beautiful pictures of regularly unfruitful ventures via telephone or through spontaneous messages. The vast majority of these fraudsters add authenticity to their pitches by alluding to speculation instructors and utilizing professionally composed handouts to pitch the endeavor.
- **Wash trading:** Wash exchanging is done to expand the action of a stock with expectations of creating the feeling that something important is coming.

- **BANK FRAUD**

Bank and saving money related fraud can happen from various perspectives from cheque fraud to credit card fraud. Perused on to find out about a portion of the diverse sorts of bank and managing an account related fakes and learn approaches to ensure your own data and keep yourself from turning into the following focus of bank and saving money related fraud.

TYPES OF BANK AND BANKING RELATED FRAUDS

- **Cheque Fraud:** Is in charge of the loss of about thousand of money yearly, which is almost 12 times the sum burglarized from banks every year. Numerous sorts of cheque tricks exist, including::
  - **Falsified Signatures:** Includes producing a mark on real limitless ticket to ride
  - **Falsified Endorsement :** Incorporates embracing and getting the money for or keeping a stolen check
  - **Forge Checks:** Is on the ascent with the headway in shading duplicating and desktop distributed
  - **Changed Checks:** where a man changes the name of the payee or dollar sum on a true blue check
  - **Check Kiting:** where a man stores a non-adequate asset register with a record, then composes another check against that sum for another record
- **Uninsured Deposits:** Happens when illegitimate organizations convince clients with high rates of interest or inshore secret to abstain from paying assessments. These organizations are not observed or approved by any government bank or monetary foundation, which means investors don't get assurance or protection on their ventures from any state or elected establishment.
- **Credit Card Fraud:** Is a regular kind of fraud that influences hundreds of thousands every year. Insights demonstrate that Master card causes five hundred million fraud harms to card organizations and charge card holders. Thus, it's savvy to figure out how to keep your charge card and bank records safe to keep credit fraud from transpiring. Also, on the off chance that you associate that you're an objective with credit fraud contact your bank or Master card organization quickly to check for fraud.

- **Falsification of Loan Applications:** Also known as financing Fraud. It happens whenever a individual generates incorrect insight to be considered for a funding, such as a home loan for their household. Occasionally, financing officers may possibly be in on the fraud.

- **INTERNET FRAUD STATISTICS AND FACTS**

The Internet gives a worldwide system of correspondence furthermore a venue for tricky showcasing and publicizing. From publicists offering you shabby product, to tricksters promising you Nigerian Money Offers, to being declared the month to month victor of an outside Lottery Club. You might think what made the main ten 2006 rundown of Internet tricks. The main ten Internet tricks as recorded by the National Consumers League's (NCL) Fraud Center, in 2006 included:

- **Online Auctions:** distorted or undelivered products or services
- **General products or services:** Misrepresented or undelivered products not obtained through deals
- **Fake Cheque Scams:** Consumers utilized fake checks to pay for sold things, and requested that have the cash wired in return
- **Nigerian Money Offers:** misleading guarantees of huge aggregates of cash, if purchasers consented to pay the exchange charge
- **Lotteries:** Asking champs to pay before guaranteeing their non-existing prize
- **Advance Fee Loans:** Request a charge from buyers in return of guaranteed individual advances
- **Phishing:** Emails putting on a show to speak to a solid source, approach purchasers for their own data (e.g. charge card number)
- **Prizes/contests:** Request an installment from purchasers with the end goal them should assert their non-existing prize
- **Internet Access Services:** Misrepresentation of the expense of Internet access and different administrations, which are frequently not gave
- **Investments:** False guarantees of increases on ventures

- **Phishing – Scams that Request Your Account Information**

"Phishing" is a type of Internet fraud that intends to take important data, for example, card numbers, client IDs and passwords. A fake site is made to appear to be like that of a honest to goodness association, regularly a money related establishment, for example, a bank or insurance agency. An email or SMS is sent asking for that the beneficiary get to the fake site and enter their own points of interest, including security access codes. The page looks real yet clients entering data are unintentionally sending their data to the fraudster.

Lasting Impact of Fraud

It is frequently indicated that a large portion of these violations, for example, protection and welfare fraud have no immediate casualties. In truth, the "harmless" methodology is the wrong approach to see the circumstance. fraud negatively affects everybody. Here are couple of outcomes we as a whole persevere:

- Monetary reduction because of direct physical harm
- Monetary reduction because of misfortunes endured by openly utilized administrations, for example, transportation, police and fire offices
- Roundabout financial misfortunes persevered by noticeable enterprises because of misfortunes endured by their customers
- Physical harm or demise to honest casualties got amidst a trick turned out badly
- Passionate and mental weights set on the misrepresentation casualties

Psychological Unrest among Victims

The enthusiastic impacts extortion can have on a casualty are maybe the most upsetting. In contrast with casualties of savage violations, they're defenseless to numerous anxiety related difficulties and mental issues. At the point when fraud develops into a considerably all the more harming wrongdoing, for example, wholesale fraud, numerous casualties think that its hard to recuperate from the monetary misfortune. In the event that they were bedeviled into a trick, they may feel as though they lost their cash, as well as their suspicion that all is well and good, self-regard and respect also. For a few, this might be a difficulty that takes years to determine.

Who is Affected by Fraud?

Fraud influences everybody. The noticeable consequence of fraud consists of:

- Bankruptcy, winding up
- Case of Bankruptcy
- Failing of suppliers' organizations
- Loss of business
- Damages to worthwhile ventures

Fraud manage with by government divisions, particularly tax fraud, cases dealt with by the significant Fraud department, Social Security fraud and fraud in the NHS, will cost you several enormous amounts every single year. In addition, an unknown percentage of fraud continues to be unreported to the authority.

Generally there tend to be always numerous undetectable prices as a outcome of fraud, such as:

- Decrease of operating time
- Reduction of company assurance
- Reduction to the Income
- enhanced insurance coverage rates
- Limited team spirits

- Possibility expenses: employees' time period
- The costs of research and prosecutions

Fraud obviously doesn't simply influence everybody; it harms the majority of them, as well. Unchecked, Fraud can possibly prompt critical individual money related results.

LITRETURE REVIEW

Ghosh and Reilly et al. (2004) [27] utilized a 3- layer, feed-forward Radial Basis Function (RBF) neural network using just two training passes required to generate a fraud rating in each two hours for the new credit card operations.

Barse et al (2003)[22] applied a multiple-layer neural network using rapid locate memory space to deal with temporary dependencies in synthetic Video-on-Demand log information.

Syeda et al (2002) [20] suggest fuzzy neural networks upon synchronous devices to increase ahead guideline manufacturing for customer- specified credit card fraud recognition.

Kim et al (2003) [23] offers SVM ensembles with both sackings and improving with collection techniques for telecom registration fraud.

Ezawa and Norton et al (1996) [3] introduced Bayesian system designs in four phases with two variables. They claim that simple regression, closest neighbor, and neural networks tend to be quite sluggish and decision trees have problems with particular individually distinct factors. The design alongside many factors and at a few dependencies carried out best for their particular telecommunications invaluable personal debt data.

Viaene et al (2004) [4] utilizes the weight of the proof system of AdaBoosted naive Bayes (boosted completely autonomous Bayesian network) rating. This enables the calculating of the general value (weight) for specific elements of suspiciousness and showing the collection of research pro and contra fraud as a stability of proof which is influenced by a straight forward additively concept.

Belhadji et al (2002) [14] decides the very best signs (attributes) of fraud by initially querying domain specialists, second computing counterfactual chances of fraud for every single indication and third Probit regressions in order to figure out the majority of important alerts. The writers also use Profit regressions in order to anticipate fraud and change the limit to match company fraud coverage on automobile assets harms.

Artis et al (1999) [9] examines a multinomial legit system (MNL) and nested multinomial logit model (NMNL) on a multiclass categorization issue. Both designs offer approximated qualified possibilities for the three classes but NMNL utilizes the two-phase evaluation for its nested option decision tree. It was practiced to automobile insurance coverage information.

Mercer et al (1990) [1] explained minimum-sections step by step simple regression evaluation for anomaly discovery on collected employee's services information.

Some other strategies consist of expert systems, association rules, and genetic development. Expert systems have actually been practiced to insurance coverage fraud.

Major and Riedinger et al (2002) [19] have accomplished a great authentic five-layer expert method in which kind of expert insights is incorporated with analytical records evaluation to recognize medical insurance protection fraud.

Pathak et al (2003) [21], ***Stefano and Gisella et al (2001)*** [15] and ***Von Altrock et al*** **(1997)** [5] have played around with fuzzy expert systems. Deshmukh and Talluru (1997) [5] practiced an expert system to administration fraud.

Chiu and Tsai et al (2004) [25] present a Fraud Patterns Mining (FPM) algorithm, customized with Apriori, to exploit a frequent structure for fraud-only credit card data.

Desirable algorithms such as neural networks, Bayesian networks, and decision trees have actually been blended or practiced in a continuous manner to enhance outcomes.

Chan et al (1999) [10] applies naive Bayes, C4.5, CART, and RIPPER because base classifiers and stacking to blend them all. They additionally analyze connecting non-complementary information units from a variety of businesses and the trimming of base classifiers. The outcomes suggest high price discount and improve performance on credit card operations.

Phua et al (2004) [26] proposes back propagation neural networks, naive Bayes, and C4.5 as base classifiers upon information partitioning taken from fraction oversampling using substitution. Its creativity is situated in the usage of a solitary meta-classifier (heap) to select the ideal base classifiers, and then blend these types of base classifiers' estimations (sacking) to develop the best expenses cost savings on automotive insurance claims.

Generally, there are substantial services on described data utilizing both the supervised and unsupervised algorithms in telecommunications fraud detection.

Cortes and Pregibon et al (2001) [17] propose the usage of signatures (telecommunication profile summaries) which kind of happen to be up-to-date day-to-day (time-driven). Fake signatures tend to be included to the exercises set and refined by monitored algorithms such as a tree, slipper, and model-averaged simple regression. The writers notice that deceptive cost-free data have a tendency to come with a considerable late overnight task and very long call intervals. Cortes and Pregibon [17] utilize signatures thought to be trustworthy to identify considerable variations in phoning activities. Association rules tend to be utilized to find out fascinating nation combos and temporary data from the earlier period. A graph-theoretical technique [39] is applied to creatively discover neighborhoods of attention of fake intercontinental call records.

Cahill et al (2002) [17] designate an averaged suspiciousness rating to each call (event-driven) dependent on its resemblance to deceptive signatures and unsimilarity to its account's regular trademark. Telephone calls with low ratings tend to be utilized to update the signature and current phone calls are adjusted a lot more intensely than previous versions in the signature.

Two researches on telecommunications information reveals that supervised strategies accomplish improved outcomes than unsupervised ones.

Moreau et al (1999) [11] reveal that supervised neural network and rule induction algorithms surpass two types of unsupervised neural networks which usually determine variations in between short-term and long-term analytical profile behaviors outlines. The very best outcomes tend to be coming from a hybrid model which blends these types of four strategies utilizing logistic regression. Utilizing true optimistic level alongside no incorrect positives as the efficiency measurement.

Taniguchi et al (1998) [8] state that supervised neural networks and Bayesian networks upon marked data accomplish considerably improve results than unsupervised strategies such as Gaussian mixture systems on every single non-fraud consumer to identify anomalous phone telephone calls.

Williams and Huang et al (1999) [12] is applicable a variety of stage procedure: k-means for cluster recognition, C4.5 for decision tree rule induction, and domain knowledge, analytical summaries as well as visualization equipment for rule analysis. Williams [12] use a genetic algorithm, alternatively of C4.5, to produce guidelines and to permit the domain individual, such as a fraud specialist, to discover the procedures and to permit all of them to develop appropriately on medical insurance claims.

Brockett et al present a comparable strategy making use of the Self-Organizing Maps (SOM) for group recognition earlier back propagation neural networks in automotive injuries claims.

Cox et al (1995)[2] utilizes an unsupervised neural network implemented by a neuron-fuzzy categorization method to supervise health care providers' claims.

Kim et al (2003) [28] executes a unique fraud recognition strategy in five steps:

1st, establish guidelines arbitrarily utilizing association rules algorithm Apriori and enhance variety by a schedule outline; 2nd, put on guidelines on understood trustworthy transaction collection, eliminate any kind of regulation which meets this particular records; 3rd, choose leftover procedures to observe real system, eliminate any rule that discovers no defects; 4th, duplicate any guideline which identifies anomalies by including little arbitrary variations; and 5th, maintain the effective rules. This strategy has already been and presently being examined for inner fraud by staff members within the retail transaction handling system.

Murad and Pinkas et al (1999) [13] utilize profiling at contact, day-to-day, and general degrees of general actions from every single telecommunications profile. The popular everyday background is produced utilizing a clustering algorithm using collective distribution distance function. An alarm is elevated if the every day profile's telephone call period, desired destination, and volume surpasses the tolerance and traditional variance of the general visibility.

Aleskerov et al (1997) [6] research with auto-associative neural networks (one undetectable layer and the exact same numbers of input and output neurons) on every credit card account's legit transactions.

Kokkinaki et al (1997) [7] proposes resemblance trees (decision trees with Boolean logic functions) to represent each trustworthy customer's activities to diagnose variances coming from the standard and group research to separate each legitimate customer's credit card transactions.

Cortes et al (2001) [17] analyzes the temporary development of large dynamic graphs' for telecommunications fraudulence discovery. Each chart is created up of subgraphs named Communities Of Interest (COI). To get over the imbalance of utilizing just the existing graph, and storage space and weight issues of utilizing all equity graphs at all time period procedures; the writers utilized the dramatically weighted frequent strategy to modify subgraphs day-to-day. Through connecting movable mobile records making use of call quantities and intervals to format COIs, the writers establish two unique faculties of fraudsters. First, deceptive mobile accounts are associated - fraudsters call every single another or the exact same mobile numbers. Second, fake call conduct from flagged fake are mirrored in some new phone accounts - fraudsters hit back with application fraud/identity crime after getting recognized.

Bolton and Hand et al (2001) [16] suggest equal Group research to supervise inter- account behavioral over time. It analyzes the collective hostile once a week quantity in between the desired profile and other comparable records (peer group) at following time period guidelines. The extended distance metric/suspiciousness rating is a figure which establishes the consistent length from the middle of the look cluster. The time period screen to determine peer group is 13 weeks and later time screen is 4 weeks on credit card records.

CONCLUSIONS

This paper gives an exhaustive review in various sort Fraud and their effect territories. It characterizes the enemy, the sorts and subtypes of Fraud, the specialized way of information, execution measurements. Subsequent to recognizing the confinements in strategies and procedures of Fraud location, this paper demonstrates that this field can profit by other related fields. After studying all kind of literature over fraud, fraud impact on different industry. Different frameworks are powerful against a few sorts of cheats, yet have some primary issues:

Firstly, they can't bolster fraud frequencies that not follow the profiles. Also, these frameworks require redesigning, to stay up with the latest with current cheats techniques. Up-evaluation and support expenses are high and mean constant reliance on framework merchants. Thirdly, they require exceptionally precise meanings of edges and parameters. There are other fascinating regions of fraud discovery, not specified in this paper, for example, voting inconsistencies, criminal exercises in e-trade, protection claims misrepresentation, guarantee fraud and misuse, and wellbeing card Fraud.

REFERENCES

1. *Mercer, L. Fraud Detection via Regression Analysis. Computers and Security 9: 331-338. 1990.*
2. *Cox, E. A Fuzzy System for Detecting Anomalous Behaviors in Healthcare Provider Claims. In Goonatilake, S. & Treleaven, P. (eds.) Intelligent Systems for Finance and Business, 111-134. John Wiley and Sons Ltd. 1995.*
3. *Ezawa, K. & Norton, S. Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts. IEEE Expert October: 45-51. 1996.*
4. *Deshmukh, A. & Talluru, T. A Rule Based Fuzzy Reasoning System for Assessing the Risk of Management Fraud. Journal of Intelligent Systems in Accounting, Finance & Management 7(4): 669-673. 1997.*
5. *Von Altrock, C. Fuzzy Logic and Neurofuzzy Applications in Business and Finance. 286- 294. Prentice Hall. 1997.*
6. *Aleskerov, E., Freisleben, B. & Rao, B. CARDWATCH: A Neural Network-Based Database Mining System for Credit Card Fraud Detection. Proc. of the IEEE/IAFE on Computational Intelligence for Financial Engineering, 220-226. 1997.*
7. *Kokkinaki, A. On Atypical Database Transactions: Identification of Probable Frauds using Machine Learning for User Profiling. Proc. of IEEE Knowledge and Data Engineering Exchange Workshop, 107-113. 1997*
8. *Taniguchi, M., Haft, M., Hollmen, J. & Tresp,. Fraud Detection in Communication Networks using Neural and Probabilistic Methods. Proc. of 1998 IEEE International Conference in Acoustics, Speech and Signal Processing, 1241- 1244. 1998.*
9. *Artis, M., Ayuso M. & Guillen M. Modelling Different Types of Automobile Insurance Fraud Behaviour in the Spanish Market. Insurance Mathematics and Economics 24: 67- 81. 1999.*
10. *Chan, P., Fan, W., Prodromidis, A. & Stolfo, S. Distributed Data Mining in Credit Card Fraud Detection. IEEE Intelligent Systems 14: 67-74. 1999.*

11. *Moreau, Y., Lerouge, E., Verrelst, H., Vandewalle, J., Stormann, C. & Burge, P. BRUTUS: A Hybrid System for Fraud Detection in Mobile Communications. Proc. of European Symposium on Artificial Neural Networks, 447-454. 1999.*

12. *Williams, G. Evolutionary Hot Spots Data Mining: An Architecture for Exploring for Interesting Discoveries. Proc. Of PAKDD99. 1999.*

13. *Murad, U. & Pinkas, G. Unsupervised Profiling for Identifying Superimposed Fraud. Proc. of PKDD99. 1999.*

14. *Belhadji, E., Dionne, G. & Tarkhani, F. A Model for the Detection of Insurance Fraud. The Geneva Papers on Risk and Insurance 25(4): 517-538. 2000.*

15. *Stefano, B. & Gisella, F. Insurance Fraud Evaluation: A Fuzzy Expert System. Proc. of IEEE International Fuzzy Systems Conference, 1491-1494. 2001.*

16. *Bolton, R. & Hand, D. Unsupervised Profiling Methods for Fraud Detection. Credit Scoring and Credit Control VII. 2001.*

17. *Cortes, C. & Pregibon, D. (2001). Signature-Based Methods for Data Streams. Data Mining and Knowledge Discovery 5: 167- 182.*

18. *Cahill, M., Chen, F., Lambert, D., Pinheiro, J. & Sun, D. Detecting Fraud in the Real World. Handbook of Massive Datasets 911-930. 2002.*

19. *Major, J. & Riedinger, D. EFD: A Hybrid Knowledge/ Statistical-based system for the Detection of Fraud. Journal of Risk and Insurance 69(3): 309-324. 2002.*

20. *Syeda, M., Zhang, Y. & Pan, Y. Parallel Granular Neural Networks for Fast Credit Card Fraud Detection. Proc. of the 2002 IEEE International Conference on Fuzzy Systems. 2002.*

21. *Pathak, J., Vidyarthi, N. & Summers, S. A Fuzzy-base Algorithm for Auditors to Detect Element of Fraud in Settled Insurance Claims, Odette School of Business Administration. 2003.*

22. *Barse, E., Kvarnstrom, H. & Jonsson, E. Synthesizing Test Data for Fraud Detection Systems. Proc. of the 19th Annual Computer Security Applications Conference, 384-395. 2003.*

23. *Kim, J., Ong, A. & Overill, R. Design of an Artificial Immune System as a Novel Anomaly Detector for Combating Financial Fraud in Retail Sector. Congress on Evolutionary Computation. 2003*

24. *Viaene, S., Derrig, R. & Dedene, G. A Case Study of Applying Boosting Naive Bayes to Claim Fraud Diagnosis. IEEE Transactions on Knowledge and Data Engineering 16(5): 612- 620. 2004.*

25. *Chiu, C. & Tsai, C. A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. Proc. of 2004 IEEE International Conference on e-Technology, e-Commerce and e- Service. 2004.*

26. *Phua, C., Alahakoon, D. & Lee. Minority Report in Fraud Detection: Classification of Skewed Data, SIGKDD Explorations 6(1): 50-59. 2004.*

27. *Ghosh, S. & Reilly, D. Credit Card Fraud Detection with a Neural Network. Proc. of 27th Hawaii International Conference on Systems Science 3: 621-630. 2004.*

28. *Kim, H., Pang, S., Je, H., Kim, D. & Bang, S. Constructing Support Vector Machine Ensemble. Pattern Recognition 36: 2757-2767. 2003.*

29. *P.Singh, B. k. Pandey, H.L.Mandoria, R. Srivastava, "Review of energy aware policy for cloud computing environment",JIT, vol. 3, 1, 14-21, Dec 2013.*

30. *Choudary S. k., Jadon R.S., H.L.Mandoria, A. Kumar, "latest development of cloud computing technology, Charactersitic, challenges, services & Application", IOSR-JCE, vol. 16, 57, 68. Nov.2014*

31. *M.Thaliyal, H.L.Mandoria, Neha Grag, "Data security analysis in Cloud Environment: A review",IJIACS, Vol.2, issues 1, 14-19, jan. 2014*

32. *Poonam Rawat, S. Dwivedi, H.L. mandoria, "An Adaptive approach in web search algorithm ", IJICT, vol.14, 2014*

33. *S. paliwal, R.S. Singh, H. L. mandoria, "Analytical Study on intrusion Detection & prevention system", IJETTCS, vol. 5, Dec. 2015.*